AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-25. (Canceled)

26. (Currently Amended) A method for protecting secret data stored in a memory of a semiconductor chip of a data carrier, said secret data serving as input data for one or more operations executed on the semiconductor chip, the execution of the one or more operations causing signals detectable from outside of the data carrier, the signals being dependent on the one or more operations and on the input data for the one or more operations, said method comprising the steps of:

- falsifying the input data by combination with auxiliary data (Z) before execution of the one or more operations (f) on the semiconductor chip,
- executing said one or more operations (f) on the semiconductor chip,
- retrieving an auxiliary function value ($f(Z)$) from said memory of said semiconductor chip of the data carrier,
- combining the output data determined by ~~execution~~ said executing of the one or more operations (f) with ~~an~~ said auxiliary function value ($f(Z)$) in order to compensate for the falsification of the input data,
- wherein the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z) in the memory of the semiconductor chip of the data carrier.

27. (Previously Presented) A method according to claim 26, wherein the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is nonlinear with respect to the combination generating the falsification.

28. (Previously Presented) A method according to claim 26, wherein the auxiliary data (Z) are varied, the corresponding function values being stored in the memory of the data carrier.

29. (Previously Presented) A method according to claim 28, wherein new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combining two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

30. (Previously Presented) A method according to claim 29, wherein the two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$) that are combined to generate the new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are each selected randomly.

31. (Previously Presented) A method according to claim 26, wherein pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

32. (Previously Presented) A method according to claim 26, wherein the auxiliary data (Z) are a random number.

33. (Previously Presented) A method according to claim 26, wherein the output data and the auxiliary function value are combined by an XOR operation.

34-41. (Canceled)

42. (Previously Presented) A method according to claim 26, wherein the operations are key permutations or permutations of other secret data.

43. (Canceled)